

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-157159

(43)Date of publication of application : 31.05.2002

(51)Int.Cl.

G06F 12/00

G06F 12/14

(21)Application number : 2000-349719

(71)Applicant : NEC CORP

(22)Date of filing : 16.11.2000

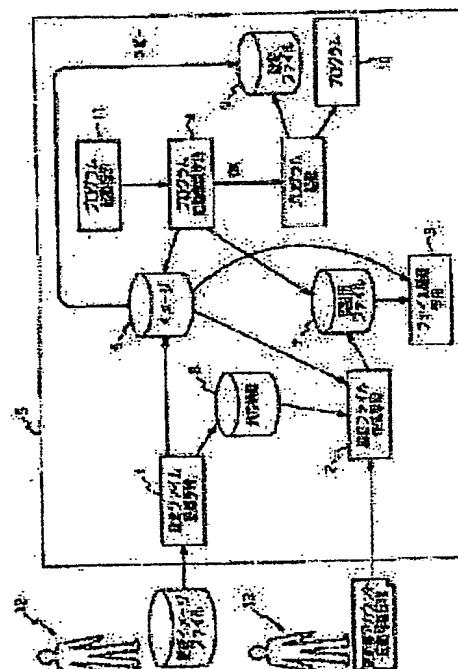
(72)Inventor : KURIMOTO AKANE

## (54) UPDATE INFORMATION PROTECTION DEVICE FOR PROGRAM START-UP SETTING FILE

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an update information protection device for a program start-up setting file preventing careless rewriting or falsification of the setting file used at the start-up time of a program to secure safety of the setting file for the program important to system operation.

**SOLUTION:** In this protection device, by registering the setting file 9 used at the start-up time of the program 10 to a disk as an image 6 and forbidding access to the disk except the start-up time of the program 10, the unjust rewriting to the image 6 that is the setting file 9 for the program start-up is prevented. When starting up the program 10, a program start-up confirmation means 4 decides the presence of the falsification of the image 6, and the program 10 is forbidden to read the image 6 as the setting file 9 when the falsification is present. Thereby, the start-up of the program 10 based on the unjust setting file is prevented.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-157159  
(P2002-157159A)

(43) 公開日 平成14年5月31日 (2002.5.31)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	ターム(参考)
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 Z 5 B 0 1 7
12/14	3 1 0	12/14	3 1 0 Z 5 B 0 8 2

審査請求 有 請求項の数 5 O L (全 7 頁)

(21) 出願番号 特願2000-349719(P2000-349719)

(22) 出願日 平成12年11月16日 (2000.11.16)

(71) 出願人 000004237

日本電気株式会社  
東京都港区芝五丁目7番1号

(72) 発明者 栗本 あかね

東京都港区芝五丁目7番1号 日本電気株  
式会社内

(74) 代理人 100079164

弁理士 高橋 勇

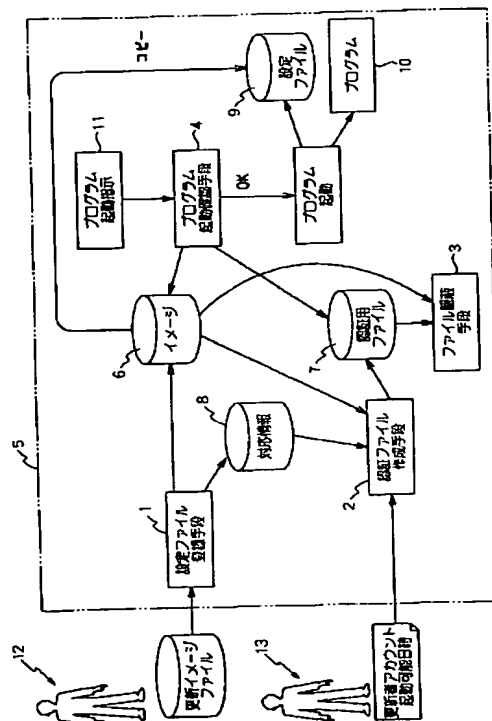
Fターム(参考) 5B017 AA02 BA06 BB09 CA16  
5B082 CA11

(54) 【発明の名称】 プログラム起動設定ファイルの更新情報保護装置

(57) 【要約】

【課題】 プログラムの起動時に使用される設定ファイルの不用意な書き替えや改竄を防止して、システムの運営上重要なプログラムの設定ファイルの安全を確保することのできるプログラム起動設定ファイルの更新情報保護装置を提供する。

【解決手段】 プログラムの起動時に使用される設定ファイルをイメージ6としてディスクに登録し、プログラムの起動時を除いて当該ディスクへのアクセスを禁止することにより、プログラム起動用の設定ファイル9となるイメージ6に対して不正な書き替えが行われるのを防止する。更に、プログラム起動時にはプログラム起動確認手段4でイメージ6の改竄の有無を判定し、改竄がある場合にはイメージ6を設定ファイル9としてプログラム10に読み込ませることを禁止することで、不正な設定ファイルに基づくプログラム10の起動を防止する。



## 【特許請求の範囲】

【請求項 1】 プログラムの起動時に使用される設定ファイルのイメージをディスクに登録する設定ファイル登録手段と、前記イメージに対する改竄の判定に用いる認証用ファイルを作成して前記ディスクに登録する認証ファイル作成手段と、前記イメージおよび認証用ファイルが格納されているディスクへのアクセスを禁止するファイル隠蔽手段と、前記プログラムに対する起動要求を検出して前記ディスクへのアクセスを許可した後、前記認証用ファイルを用いて前記イメージに対する改竄の有無を判定し、改竄がない場合に限り前記イメージを前記プログラムの起動時に使用される設定ファイルのディレクトリに設定ファイルとして配置し、この設定ファイルに基いて前記プログラムを起動する一方、改竄があった場合には前記ディレクトリへのイメージの配置と前記プログラムの起動を禁止するプログラム起動確認手段とを備えたことを特徴とするプログラム起動設定ファイルの更新情報保護装置。

【請求項 2】 前記設定ファイル登録手段は、前記イメージを作成または更新した日時を特定する日時データと前記イメージとの対応関係を記録した対応情報を前記ディスクに登録する機能を有し、前記認証ファイル作成手段は、前記ディスクに登録された対応情報から前記イメージと前記日時データとの対応関係を読み込んで前記認証用ファイルに設定する機能を有し、前記プログラム起動確認手段は、前記ディスクに記録された日付データと前記認証用ファイルに設定された日付データとを比較して、両者が一致した場合に限り前記イメージに対する改竄がないものと判定するように構成されていることを特徴とした請求項 1 記載のプログラム起動設定ファイルの更新情報保護装置。

【請求項 3】 前記設定ファイル登録手段は、前記イメージを作成または更新したユーザを特定するユーザアカウントと前記イメージとの対応関係を記録した対応情報を前記ディスクに登録する機能を有し、前記認証ファイル作成手段は、前記イメージとプログラム起動アカウントとの対応関係を前記認証用ファイルに設定する機能を有し、前記プログラム起動確認手段は、前記ディスクに記録されたユーザアカウントと前記認証用ファイルに設定されたプログラム起動アカウントとを比較して、両者が一致した場合に限り前記イメージに対する改竄がないものと判定するように構成されていることを特徴とした請求項 1 または請求項 2 記載のプログラム起動設定ファイルの更新情報保護装置。

【請求項 4】 前記認証ファイル作成手段は、前記イメージを設定ファイルとして利用するプログラムの起動可能日時と前記イメージとの対応関係を前記認証用ファイルに設定する機能を有し、前記プログラム起動確認手段は、前記認証用ファイルに設定された起動可能日時と現在時刻とを比較して、両者が一致した場合に限り前記

イメージに対する改竄がないものと判定するように構成されていることを特徴とした請求項 1、請求項 2 または請求項 3 記載のプログラム起動設定ファイルの更新情報保護装置。

【請求項 5】 オペレーティングシステムが備えるアクセス禁止コマンドによって前記ファイル隠蔽手段が構成されていることを特徴とした請求項 1、請求項 2、請求項 3 または請求項 4 記載のプログラム起動設定ファイルの更新情報保護装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、プログラムの起動時に使用される設定ファイルの改竄や不要な書き換えを防止するプログラム起動設定ファイルの更新情報保護装置に関する。

## 【0002】

【従来技術】 プログラムの不正使用を防止するための防衛手段としては、例えば、特開平 6-223040 号に開示されるように、プログラムのライセンス数に基いてプログラムの過剰な同時使用を禁止するもの、あるいは、特開平 8-305559 号に開示されるように、セーブ日時やプログラム番号および計算機の識別番号に基いてアプリケーションの不正な立ち上げを禁止するものが知られている。

## 【0003】

【発明が解決しようとする課題】 しかし、これらの従来技術は飽くまでプログラム本体の不正使用を防止するためのものであり、プログラムの使用環境を決める設定ファイルの保護に関しては全く考慮されていない。

【0004】 このため、ファイル転送等によって容易にファイルの書き換えを行うことが可能な UNIX（登録商標）等のオープンシステムにおいては、ファイル転送等によって不用意に設定ファイルの内容が書き換えられる可能性があり、システムの運営上重要なプログラム、例えば、ミドルウェアやアプリケーションの設定ファイルの安全が確保されにくいといった問題が生じる場合がある。

## 【0005】

【発明の目的】 そこで、本発明の目的は、前記従来技術の欠点を解消し、プログラムの起動時に使用される設定ファイルの不要な書き換えや改竄を防止して、システムの運営上重要なプログラムの設定ファイルの安全を確保することのできるプログラム起動設定ファイルの更新情報保護装置を提供することにある。

## 【0006】

【課題を解決するための手段】 本発明は、プログラムの起動時に使用される設定ファイルのイメージをディスクに登録する設定ファイル登録手段と、前記イメージに対する改竄の判定に用いる認証用ファイルを作成して前記ディスクに登録する認証ファイル作成手段と、前記イメ

10

20

30

40

50

ージおよび認証用ファイルが格納されているディスクへのアクセスを禁止するファイル隠蔽手段と、前記プログラムに対する起動要求を検出して前記ディスクへのアクセスを許可した後、前記認証用ファイルを用いて前記イメージに対する改竄の有無を判定し、改竄がない場合に限り前記イメージを前記プログラムの起動時に使用される設定ファイルのディレクトリに設定ファイルとして配置し、この設定ファイルに基いて前記プログラムを起動する一方、改竄があった場合には前記ディレクトリへのイメージの配置と前記プログラムの起動を禁止するプログラム起動確認手段とを備えたことを特徴とする構成により前記目的を達成した。

【0007】設定ファイル登録手段は、プログラムの起動時に使用される設定ファイルのイメージをディスクに登録し、また、認証ファイル作成手段は、イメージに対する改竄の判定に用いる認証用ファイルを作成してディスクに登録する。イメージが格納されているディスクへのアクセスはファイル隠蔽手段によって禁止されているので、設定ファイルのイメージの内容がオープンシステムのファイル転送等によって不用意に書き替えられることはなく、また、外部からのアクセスによる不正な書き替えの心配もない。更に、システム管理者や一般ユーザが設定ファイルのイメージや認証用ファイルのディレクトリを特定することも困難であるので、システム管理者や一般ユーザからの不正操作によるイメージや認証用ファイルの改竄も防止される。プログラム起動確認手段は、プログラムに対する起動要求を検出して初めて、イメージと認証用ファイルを格納したディスクへのアクセスを許可し、認証用ファイルを用いて前記イメージに対する改竄の有無を判定する。この段階でイメージに対する改竄が検出された場合には、この設定ファイルのイメージは飽くまでイメージのまま保持され、このイメージが、プログラムの起動時に使用される設定ファイルのディレクトリに移動されることはない。この場合、プログラムの起動も同時に禁止される。従って、仮に、イメージに改竄が施されていたとしても、このイメージが設定ファイルとしてプログラムに読み込まれることはなく、不正な設定ファイルに基くプログラムの起動が未然に防止されることになる。これにより、システムの運営上重要なプログラム、例えば、ミドルウェアやアプリケーション等の誤動作が防止され、安全な処理動作が保証される。また、イメージに対する改竄が検出されなければ、プログラム起動確認手段は、プログラムの起動時に使用される設定ファイルのディレクトリに前記イメージを設定ファイルとして配置し、この段階で初めて、前記イメージが実質的な設定ファイルとして機能することを許容する。この場合、プログラム起動確認手段は、正規のディレクトリに配置された設定ファイルに基いて前記プログラムを起動し、このプログラムを使用した作業の開始を許容する。

【0008】ここで、設定ファイル登録手段には、イメージを作成または更新した日時を特定する日時データとイメージとの対応関係を記録した対応情報をディスクに登録する機能を持たせ、また、認証ファイル作成手段には、ディスクに登録された対応情報からイメージと日時データとの対応関係を読み込んで認証用ファイルに設定する機能を持たせることができる。対応情報はイメージと一体化しても構わない。この場合、プログラム起動確認手段は、ディスクに对应情報として登録された日付データと認証用ファイルに設定された日付データとを比較して、両者が一致した場合に限りイメージに対する改竄がないものと判定するように構成する。

【0009】このような構成によれば、認証ファイル作成後の不正操作によって改竄されたイメージが設定ファイルとして機能したり、不正なイメージを設定ファイルとして使用したプログラムの起動を未然に防止することができる。

【0010】また、イメージを作成または更新したユーザを特定するユーザアカウントとイメージとの対応関係を記録した対応情報をディスクに登録する機能を設定ファイル登録手段に持たせ、認証ファイル作成手段には、イメージとプログラム起動アカウントとの対応関係を認証用ファイルに設定する機能を持たせることができる。対応情報はイメージと一体化しても構わない。この場合、プログラム起動確認手段は、ディスクに对应情報として登録されたユーザアカウントと認証用ファイルに設定されたプログラム起動アカウントとを比較し、両者が一致した場合に限りイメージに対する改竄がないものと判定するように構成する。

【0011】これにより、プログラムを起動する使用権のないユーザが作成または更新したイメージが設定ファイルとして機能したり、不正なイメージを設定ファイルとして使用したプログラムの起動を未然に防止することができる。

【0012】更に、プログラムの起動可能日時とイメージとの対応関係を認証用ファイルに設定する機能を認証ファイル作成手段に持たせ、認証用ファイルに設定された起動可能日時と現在時刻とを比較して、両者が一致した場合に限りイメージに対する改竄がないものと判定するようにプログラム起動確認手段を構成することも可能である。

【0013】このような構成によれば、予め設定された日時以外にプログラムが不正に起動されるのを防止することができる。

【0014】また、ファイル隠蔽手段は、オペレーティングシステムが備えるアクセス禁止コマンドを利用して構成することができる。

【0015】オペレーティングシステムが備えるアクセス禁止コマンドを利用することにより、設定ファイルのイメージおよび認証用ファイルを容易に隠蔽することが

10

20

30

40

50

可能となる。

#### 【0016】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態について詳細に説明する。図1は本発明を適用した一実施形態のプログラム起動設定ファイルの更新情報保護装置の構成の概略を示した機能ブロック図である。

【0017】このうち、更新情報保護装置の主要部を形成する設定ファイル登録手段1と認証ファイル作成手段2およびファイル隠蔽手段3とプログラム起動確認手段4の各々は、実質的に、オープンシステム5内、例えば、UNIXマシン内に設置されたプログラムによって構成される。

【0018】設定ファイル登録手段1で作成された設定ファイルのイメージ6と対応情報8、および、認証ファイル作成手段2で作成された認証用ファイル7は、オープンシステム5内のディスク、つまり、ハードディスク等の記憶装置に格納される。

【0019】また、ファイル隠蔽手段3は、オープンシステム5のオペレーティングシステムが標準的に備えるアクセス禁止コマンド、例えば、HP-UXにおけるvgreduceコマンド等を使用して、イメージ6、認証用ファイル7、対応情報8を格納したディスクへの外部および内部からのアクセスを禁止するようになっている。

【0020】設定ファイル登録手段1は、プログラムの起動時に使用される設定ファイルの作成あるいは更新の際に使用されるが、ここで作成された設定ファイルは、プログラムの起動時に設定ファイルの読み込みに使用されるディレクトリ、つまり、図1に示されるような設定ファイル9の位置には直ちに配置されず、前述したアクセス禁止の設定が可能なディスク内にそのまま保持される。

【0021】この実施形態では、プログラムの起動時に設定ファイルの読み込みに使用されるディレクトリに置かれた設定ファイル、要するに、実際にプログラムの立ち上げに使用される設定ファイルを設定ファイル9と呼び、また、アクセス禁止の設定が可能なディスク内に保持された設定ファイルのことを単にイメージ6と呼んでいる。設定ファイル登録手段1で作成された設定ファイルのイメージ6が適切なものである限り、実質的に、イメージ6と設定ファイル9の内容は同一である。

【0022】ここでいう設定ファイルとは、例えば、プログラムの実行に必要なとされるパラメータを保存したファイル、あるいは、複数の一般ユーザが同一プログラムを使用する際に使用する各ユーザ毎の環境設定ファイル等である。

【0023】プログラム起動確認手段4には、ミドルウェアやアプリケーション等のプログラム10を起動するためのイベントであるプログラム起動指示11を検出してディスクに対するアクセス禁止設定を解除し、イメー

ジ6、認証用ファイル7、対応情報8にアクセスする機能があり、このプログラム起動指示11を検出した段階で、プログラム起動確認手段4が前述した認証用ファイル7を使用してイメージ6に対する改竄の有無を判定する。

【0024】そして、改竄がないと判定された場合に限り、プログラム起動確認手段4は、イメージ6を設定ファイルの正規のディレクトリ、つまり、図1に示される9の位置にコピーして、このコピー（イメージ）を正規の設定ファイル9とし、この設定ファイル9の内容に基づいてプログラム10を起動する。

【0025】また、改竄があると判定された場合には、プログラム起動確認手段4は、正規のディレクトリへのイメージ6のコピーを非実行とし、プログラム10の起動も禁止する。

【0026】以下、図1の機能ブロック図と各手段の処理動作の概略を示した図2～図4のフローチャートを参照して、本実施形態の更新情報保護装置の処理動作について詳細に説明する。

【0027】図2は設定ファイル登録手段によって実行される設定ファイル登録処理について示したフローチャートである。

【0028】まず、一般ユーザ12がパラメータや環境設定関係等の設定ファイルを作成あるいは更新し、この設定ファイルをユーザアカウント（ユーザを識別するためのコード）と共に設定ファイル登録手段1に入力する（ステップa1）。設定ファイルの作成あるいは更新を行う一般ユーザは単数であっても複数であっても構わない。

【0029】設定ファイル登録手段1は、入力された設定ファイルをイメージ6としてディスクに格納し（ステップa2）、更に、今回作成されたイメージ6とこれを作成したユーザおよび現在時刻との対応関係を記憶した対応情報8を作成してディスクに格納する（ステップa3）。この場合のユーザとは具体的にはユーザアカウントの値である。また、ユーザアカウントおよび現在時刻はイメージ6自体にも添付される。

【0030】次に、認証ファイル作成手段2を利用したシステム管理者側の作業が行われることになる。

【0031】図3は認証ファイル作成手段2によって実行される認証用ファイル作成処理について示したフローチャートである。

【0032】システム管理者13は、まず、認証ファイル作成手段2を用いて、プログラムの起動可能日時とユーザアカウント（この場合は一般ユーザ12のユーザアカウント）等を入力する（ステップb1）。

【0033】すると、この入力操作を検出した認証ファイル作成手段2は、システム管理者13が入力したユーザアカウントに基づいてディスク内の対応情報を検索し、該当する一般ユーザ12の対応情報8を抽出して、イメ

ージ6の情報と該イメージ6の作成日時（イメージ作成時に記録された現在時刻）を取得し（ステップb2）、モニタ画面に一般ユーザ12が作成したイメージ6の内容、つまり、一般ユーザ12が作成あるいは更新した設定ファイルの内容を表示する（ステップb3）。

【0034】次いで、システム管理者13は、モニタ画面に表示された設定ファイルの内容を確認し、問題がなければ、このイメージ6を設定ファイル9として使用することを許諾し、認証ファイル作成手段2による認証用ファイル7の作成を実行させる（ステップb4）。この認証用ファイル7には、イメージ6の作成日時と、このイメージ6を作成あるいは更新した一般ユーザ12のユーザアカウント（プログラム起動アカウント）、および、前述したステップb1の処理でシステム管理者13が設定したプログラムの起動可能日時が記録される。

【0035】そして、認証ファイル作成手段2はファイル隠蔽手段3を動作させ、設定ファイル登録手段1によって作成されたイメージ6と認証ファイル作成手段2によって作成された認証用ファイル7の格納されているディスクをオペレーティングシステムの機能、例えば、HP-UXにおけるvgreduceコマンド等を使用してアクセスできない状態にする（ステップb5）。

【0036】次に、図4に示す起動確認処理のフローチャートを参照してプログラム起動確認手段4の処理動作について説明する。

【0037】プログラム10を起動するためのイベントであるプログラム起動指示11がプログラム起動確認手段4によって検出されると、プログラム起動確認手段4は、まず、ファイル隠蔽手段3によるアクセス禁止設定をオペレーティングシステムの機能、例えば、HP-UXにおけるvgextendコマンド等を使用して解除し（ステップc1）、当該プログラム10の起動に必要とされる設定ファイル9に対応するイメージ6を参照して（ステップc2）、このイメージ6に添付された作成日付と認証用ファイル7に記録されたイメージ6の作成日付とが一致しているか否かを判定する（ステップc3）。

【0038】更に、両者が一致している場合には、当該プログラム10の起動に必要とされる設定ファイル9に対応するイメージ6の認証用ファイル7を参照して（ステップc4）、認証用ファイル7に記録された起動可能日時と現在時刻、および、認証用ファイル7に記録されたプログラム起動アカウントとイメージ6に添付されたユーザアカウントとを比較する（ステップc5）。

【0039】そして、作成日付、起動可能日時、ユーザアカウントの全てが一致した場合にはイメージ6に不適当な改竄がないものと判定し、プログラム起動確認手段4は、図1に示されるようにして、プログラム10の起動に必要とされる設定ファイル9に対応するイメージ6を正規のディレクトリにコピーして設定ファイル9を生成し（ステップc6）、この設定ファイル9の設定、例

えば、パラメータや環境設定等を利用してプログラム10を起動した後、再びファイル隠蔽手段3を使用して、ディスクに対するアクセスを禁止の状態とする。

【0040】一方、ステップc3あるいはステップc5の判定処理において、作成日付、起動可能日時、ユーザアカウントの何れかに不一致が認められた場合には、プログラム起動確認手段4は、イメージ6に不適切な改竄があるものと判定し、ステップc6におけるイメージのコピー処理を非実行として、プログラム10の起動も禁止する（ステップc7）。

【0041】以上に述べた通り、設定ファイルのイメージ6が格納されているディスクへのアクセスは、プログラム10の起動時を除き、ファイル隠蔽手段3によって常に禁止の状態とされているので、一旦設定されたイメージ6の内容がファイル転送等によって不用意に書き替えられることはなく、また、外部からのアクセスによる不正な書き替えの心配もない。更に、システム管理者13や一般ユーザ12がイメージ6や認証用ファイル7のディレクトリを特定することも事実上不可能であるので、システム管理者13や一般ユーザ12からの不正操作によるイメージ6や認証用ファイル7の改竄も未然に防止される。

【0042】プログラム起動確認手段4は、プログラム10に対するプログラム起動指示11を検出して初めて、イメージ6と認証用ファイル7を格納したディスクへのアクセスを許可し、イメージ6に不適当な改竄がない場合に限ってイメージ6をプログラム起動用の正規のディレクトリにコピーして設定ファイル9としての使用を許可する一方、イメージ6に不適当な改竄が認められた場合には、イメージ6のコピー処理、つまり、イメージ6を設定ファイル9として使用することを禁止するようにしているので、仮に、イメージ6に改竄が施されていたとしても、このイメージ6が設定ファイル9としてプログラム10に読み込まれることはなく、不正な設定ファイルに基づくプログラム10の起動が未然に防止される。よって、システムの運営上重要なプログラム、例えば、ミドルウェアやアプリケーション等の安全が処理動作が確保される。

【0043】また、イメージ6の改竄の判定に用いるデータとしては、イメージ6の作成日付およびプログラム10の起動可能日時とプログラム起動アカウントとを並列的に利用するようにしているので、認証ファイル7を作成した後の不正操作によるイメージ6の改竄や、規定時間外のプログラム10の不正な立ち上げ、更には、プログラム10を起動する使用権のないユーザ12によるプログラム10の不正使用も未然に防止することができる。

【0044】イメージ6の改竄の判定に用いるデータとしては、前述した作成日付、起動可能日時、プログラム起動アカウントの他にも、イメージ6のファイルサイズ

10

20

30

40

50

や有効時間等を利用することが可能である。

【0045】イメージ6のファイルサイズを判定データとして利用する場合には、イメージ6の作成時にそのファイルサイズを測定してイメージ6に添付すると共に、このファイルサイズを認証用ファイル7にも記録する。そして、プログラム起動指示11が検出された時点で、イメージ6のファイルサイズを再び測定して認証用ファイル7に記録されているファイルサイズと比較し、ファイルサイズの一致不一致によってイメージ6の改竄の有無を判定するようにする。

【0046】有効時間を判定データとして利用する場合の処理に関しては、前述した起動可能日時の場合と同様である。

【0047】また、イメージ6の作成時にイメージ6自体のコピーを保存しておき、プログラム10の起動時にイメージ6とそのコピーとを直接比較したり、あるいは、差分の有無を測定することによって改竄の有無を判定するようにしてもよい。

【0048】

【発明の効果】本発明によるプログラム起動設定ファイルの更新情報保護装置は、プログラムの起動時に使用される設定ファイルをイメージとしてディスクに登録し、プログラムの起動時を除いて当該ディスクへのアクセスを禁止するようにしているので、設定ファイルのイメージの内容がオープンシステムのファイル転送等によって不用意に書き替えられることはなく、また、外部からのアクセスによる不正な書き替えも未然に防止することができる。また、ディスクへのアクセスが禁止される結果、システム管理者や一般ユーザが設定ファイルのイメージのあるディレクトリを特定することも事実上不可能であり、システム管理者や一般ユーザからの不正操作によるイメージの改竄や上書きも防止される。更に、プログラム起動確認手段は、プログラムに対する起動要求を検出して初めて、イメージを格納したディスクへのアクセスを許可し、認証用ファイルを用いてイメージに対する改竄の有無を判定すると共に、イメージに改竄がない場合に限ってイメージを正規のディレクトリに配置してプログラム起動用の設定ファイルとする一方、イメージに改竄が検出された場合には、このイメージを設定ファイルのディレクトリに移動することを禁止し、同時に、プログラムの起動も禁止するようにしているので、仮に、イメージに改竄が施されていたとしても、このイメージが設定ファイルとしてプログラムに読み込まれることはなく、不正な設定ファイルに基づくプログラムの起動

を未然に防止することができる。従って、システムの運営上重要なプログラム、例えば、ミドルウェアやアプリケーション等の安全な処理動作を確保することができる。

【0049】特に、イメージを作成または更新した日時を特定する日時データや、イメージを作成または更新したユーザを特定するユーザアカウント、更には、プログラムの使用を許可する起動可能日時を改竄判定のデータとして適用することにより、認証ファイル作成後の不正操作によって改竄されたイメージの不正使用や、プログラムを起動する使用権のないユーザによるプログラムの不正使用、および、時間外のプログラムの不正使用を確実に防止することができる。

【0050】更に、ファイル隠蔽手段は、オペレーティングシステムが備えるアクセス禁止コマンドを利用してディスクを隠蔽するようにしているので、複雑なプログラムを作成することなく、設定ファイルのイメージや認証用ファイルを確実に隠蔽することができる。

【図面の簡単な説明】

【図1】本発明を適用した一実施形態のプログラム起動設定ファイルの更新情報保護装置の構成の概略を示した機能ブロック図である。

【図2】設定ファイル登録手段によって実行される設定ファイル登録処理について示したフローチャートである。

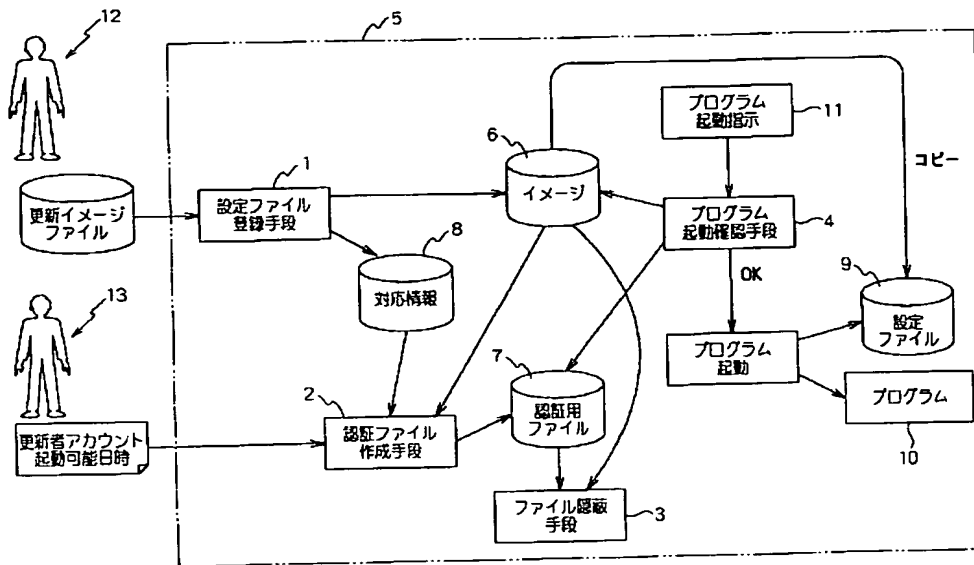
【図3】認証ファイル作成手段によって実行される認証用ファイル作成処理について示したフローチャートである。

【図4】プログラム起動確認手段によって実行される起動確認処理について示したフローチャートである。

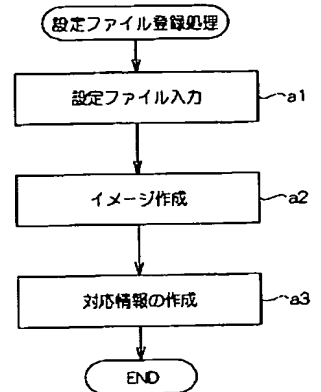
【符号の説明】

- 1 設定ファイル登録手段
- 2 認証ファイル作成手段
- 3 ファイル隠蔽手段
- 4 プログラム起動確認手段
- 5 オープンシステム
- 6 設定ファイルのイメージ
- 7 認証用ファイル
- 8 対応情報
- 9 設定ファイル
- 10 プログラム
- 11 プログラム起動指示
- 12 一般ユーザ
- 13 システム管理者

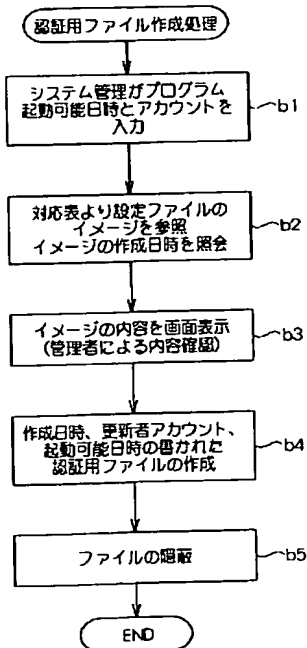
【図1】



【図2】



【図3】



【図4】

